

WHAT IS CLAIMED IS:

1. An information recording apparatus for recording reproducing
limit information for controlling reproducing manner of recording
5 information which is encrypted and supplied from an external source
to be recorded in a recording medium, together with the recording
information, into the recording medium, said apparatus comprising:

an adding device for adding the reproducing limit information
to the supplied recording information to generate added recording
10 information;

an embedding device for embedding the reproducing limit
information on the recording information within the generated added
recording information in a way of preventing from illegal detection to
generate embedded recording information; and

15 a recording device for recording the generated embedded
recording information into the recording medium.

2. The information recording apparatus according to Claim 1,
wherein

20 the embedding device embeds correspondence information
corresponding to the reproducing limit information in one-to-one and
having smaller information amount than the reproducing limit
information, on the recording information, in a way of preventing
from illegal detection to generate the embedded recording information.

25 3. The information recording apparatus according to Claim 1,
wherein

the embedding device comprises:

30 a replacement information generating device for generating
replacement information by using the reproducing limit information;
and

a replacing device for replacing one part of the recording information with the generated replacement information to generate the embedded recording information.

5 4. The information recording apparatus according to Claim 1, further comprising:

a detecting device for detecting identification information particular to each recording medium and previously recorded in the recording medium, prior to the recording of the embedded recording information; and

a key information generating device for generating key information for encrypting cryptographic information used for encrypting the recording information, by using the detected identification information, wherein

15 the embedding device embeds the generated key information on start information detected at starting the reproducing of the recording information to generate embedded start information, prior to the recording of the embedded recording information, and

20 the recording device records the generated embedded start information into a start information recording area that is an area on the recording medium where the start information is to be recorded, prior to the recording of the embedded recording information.

25 5. The information recording apparatus according to Claim 4, further comprising:

a detecting device for detecting the key information from the start information recording area when recording the embedded recording information into the recording medium; and

30 a cryptographic information encrypting device for encrypting the cryptographic information by using the key information to generate encrypted cryptographic information, wherein

the adding device adds the reproducing limit information and the encrypted cryptographic information to the recording information when recording the embedded recording information into the recording medium to generate the added recording information.

5

6. The information recording apparatus according to Claim 1, further comprising:

a detecting device for detecting identification information particular to each recording medium and previously recorded in the recording medium, prior to the recording of the embedded recording information; and

10

a key information generating device for generating key information for encrypting cryptographic information used for encrypting the recording information, by using the detected identification information, wherein

15

the embedding device embeds the generated key information on content information indicating the content of the recording information to generate embedded content information, prior to the recording of the embedded recording information, and

20

the recording device records the generated embedded content information in the recording medium.

7. The information recording apparatus according to Claim 6, further comprising:

a detecting device for detecting the key information from the recording medium when recording the embedded recording information into the recording medium; and

25

a cryptographic information encrypting device for encrypting the cryptographic information by using the key information to generate the encrypted cryptographic information, wherein

30

the adding device adds the reproducing limit information and the encrypted cryptographic information to the recording information to generate the added recording information, when recording the embedded recording information into the recording medium.

5

8. An information reproducing apparatus for reproducing recording information, which is encrypted and recorded with an reproducing limit information for controlling reproducing manner of the recording information in a recording medium, based on the reproducing limit information, said reproducing limit information which is added to the recording information and also embedded on the recording information in a way of preventing from illegal detection, said information reproducing apparatus comprising:

10

a reproducing limit information detecting device for detecting

15

the added reproducing limit information;

a reproducing limit information extracting device for extracting the embedded reproducing limit information from the recording information;

a recording information extracting device for extracting original recording information from the recording information on which the reproducing limit information is embedded; and

20

an output control device for, only when the detected reproducing limit information matches the extracted reproducing limit information, supplying the extracted original recording information based on the reproducing limit information.

25

9. The information reproducing apparatus, according to Claim 8, wherein

said recording medium having a start information recording area, said start information recording area in which start information detected at starting the reproducing of the recording information is

30

recorded, said start information on which key information for encrypting cryptographic information used for encrypting the recording information is embedded, said key information which is generated by using identification information, said identification information particular to each recording medium and recorded in the recording medium, said cryptographic information which is encrypted by using the key information and added to the recording information to which the reproducing limit information is added,

wherein said information reproducing apparatus further comprises:

a key information detecting device for detecting the key information from the start information recording area;

an encrypted cryptographic information detecting device for detecting the encrypted cryptographic information from the recording medium;

an obtaining device for decoding the detected encrypted cryptographic information by using the detected key information and obtaining original cryptographic information; and

a decoding device for decoding the extracted original recording information by using the obtained original cryptographic information and supplying the decoded recording information to the output control device.

10. The information reproducing apparatus, according to Claim 8, wherein

said recording medium in which content information indicating the content of the recording information is recorded, said content information on which key information for encrypting cryptographic information used for encrypting the recording information is embedded, said key information which is generated by using identification information, said identification information particular

to each recording medium and recorded in the recording medium, said cryptographic information which is encrypted by using the key information and added to the recording information to which the reproducing limit information is added,

5 wherein said information reproducing apparatus further comprises:

a key information detecting device for detecting the key information from the recording medium;

10 an encrypted cryptographic information detecting device for detecting the encrypted cryptographic information from the recording medium;

an obtaining device for decoding the detected encrypted cryptographic information by using the detected key information and obtaining original cryptographic information; and

15 a decoding device for decoding the extracted original recording information by using the obtained original cryptographic information and supplying the decoded recording information to the output control device.

20 11. An information recording method for recording reproducing limit information for controlling reproducing manner of recording information which is encrypted and supplied from an external source to be recorded in a recording medium, together with the recording information, into the recording medium, said method comprising:

25 an adding process for adding the reproducing limit information to the supplied recording information to generate added recording information;

30 an embedding process for embedding the reproducing limit information on the recording information within the generated added recording information in a way of preventing from illegal detection to generate embedded recording information; and

a recording process for recording the generated embedded recording information into the recording medium.

12. The information recording method according to Claim 11,
5 wherein

the embedding process embeds correspondence information corresponding to the reproducing limit information in one-to-one and having smaller information amount than the reproducing limit information, on the recording information, in a way of preventing
10 from illegal detection to generate the embedded recording information.

13. The information recording method according to Claim 11,
wherein

the embedding process comprises:

15 a replacement information generating process for generating replacement information by using the reproducing limit information;
and

a replacing process for replacing one part of the recording information with the generated replacement information to generate
20 the embedded recording information.

14. The information recording method according to Claim 11,
further comprising:

a detecting process for detecting identification information
25 particular to each recording medium and previously recorded in the recording medium, prior to the recording of the embedded recording information; and

a key information generating process for generating key information for encrypting cryptographic information used for
30 encrypting the recording information, by using the detected identification information, wherein

the embedding process embeds the generated key information on start information detected at starting the reproducing of the recording information to generate embedded start information, prior to the recording of the embedded recording information, and

5 the recording process records the generated embedded start information into a start information recording area that is an area on the recording medium where the start information is to be recorded, prior to the recording of the embedded recording information.

10 15. The information recording method according to Claim 14, further comprising:

a detecting process for detecting the key information from the start information recording area when recording the embedded recording information into the recording medium; and

15 a cryptographic information encrypting process for encrypting the cryptographic information by using the key information to generate encrypted cryptographic information, wherein

the adding process adds the reproducing limit information and the encrypted cryptographic information to the recording information
20 when recording the embedded recording information into the recording medium to generate the added recording information.

16. The information recording method according to Claim 11, further comprising:

25 a detecting process for detecting identification information particular to each recording medium and previously recorded in the recording medium, prior to the recording of the embedded recording information; and

a key information generating process for generating key
30 information for encrypting cryptographic information used for

encrypting the recording information, by using the detected identification information, wherein

the embedding process embeds the generated key information on content information indicating the content of the recording information to generate embedded content information, prior to the recording of the embedded recording information, and

the recording process records the generated embedded content information in the recording medium.

17. The information recording method according to Claim 16, further comprising:

a detecting process for detecting the key information from the recording medium when recording the embedded recording information into the recording medium; and

a cryptographic information encrypting process for encrypting the cryptographic information by using the key information to generate the encrypted cryptographic information, wherein

the adding process adds the reproducing limit information and the encrypted cryptographic information to the recording information to generate the added recording information, when recording the embedded recording information into the recording medium.

18. An information reproducing method for reproducing recording information, which is encrypted and recorded with an reproducing limit information for controlling reproducing manner of the recording information in a recording medium, based on the reproducing limit information, said reproducing limit information which is added to the recording information and also embedded on the recording information in a way of preventing from illegal detection, said method comprising:

a reproducing limit information detecting process for detecting the added reproducing limit information;

a reproducing limit information extracting process for extracting the embedded reproducing limit information from the recording information;

a recording information extracting process for extracting original recording information from the recording information on which the reproducing limit information is embedded; and

an output control process for, only when the detected reproducing limit information matches the extracted reproducing limit information, supplying the extracted original recording information based on the reproducing limit information.

19. The information reproducing method, according to Claim 18, wherein

said recording medium having a start information recording area, said start information recording area in which start information detected at starting the reproducing of the recording information is recorded, said start information on which key information for encrypting cryptographic information used for encrypting the recording information is embedded, said key information which is generated by using identification information, said identification information particular to each recording medium and recorded in the recording medium, said cryptographic information which is encrypted by using the key information and added to the recording information to which the reproducing limit information is added,

wherein said information reproducing method further comprises:

a key information detecting process for detecting the key information from the start information recording area;

an encrypted cryptographic information detecting process for detecting the encrypted cryptographic information from the recording medium;

an obtaining process for decoding the detected encrypted cryptographic information by using the detected key information and obtaining original cryptographic information; and

a decoding process for decoding the extracted original recording information by using the obtained original cryptographic information and supplying the decoded recording information to the output control process.

20. The information reproducing method, according to Claim 18, wherein

said recording medium in which content information indicating the content of the recording information is recorded, said content information on which key information for encrypting cryptographic information used for encrypting the recording information is embedded, said key information which is generated by using identification information, said identification information particular to each recording medium and recorded in the recording medium, said cryptographic information which is encrypted by using the key information and added to the recording information to which the reproducing limit information is added,

wherein said information reproducing method further comprises:

a key information detecting process for detecting the key information from the recording medium;

an encrypted cryptographic information detecting process for detecting the encrypted cryptographic information from the recording medium;

an obtaining process for decoding the detected encrypted cryptographic information by using the detected key information and obtaining original cryptographic information; and

a decoding process for decoding the extracted original recording information by using the obtained original cryptographic information and supplying the decoded recording information to the output control process.

21. An information recording medium in which a recording control program is recorded in a readable way by a recording computer included in an information recording apparatus for recording reproducing limit information for controlling reproducing manner of recording information which is encrypted and supplied from an external source to be recorded in a recording medium, together with the recording information, into the recording medium, said recording program causing the recording computer to function as:

an adding device for adding the reproducing limit information to the supplied recording information to generate added recording information;

an embedding device for embedding the reproducing limit information on the recording information within the generated added recording information in a way of preventing from illegal detection to generate embedded recording information; and

a recording device for recording the generated embedded recording information into the recording medium.

22. The information recording medium, according to Claim 21, wherein

the embedding device embeds correspondence information corresponding to the reproducing limit information in one-to-one and having smaller information amount than the reproducing limit

information, on the recording information, in a way of preventing from illegal detection to generate the embedded recording information.

23. The information recording medium, according to Claim 21,
5 wherein

the embedding device comprises:

a replacement information generating device for generating replacement information by using the reproducing limit information; and

10 a replacing device for replacing one part of the recording information with the generated replacement information to generate the embedded recording information.

24. The information recording medium according to Claim 21,
15 wherein said recording program causes the recording computer to further function as:

a detecting device for detecting identification information particular to each recording medium and previously recorded in the recording medium, prior to the recording of the embedded recording
20 information; and

a key information generating device for generating key information for encrypting cryptographic information used for encrypting the recording information, by using the detected identification information, wherein

25 the embedding device embeds the generated key information on start information detected at starting the reproducing of the recording information to generate embedded start information, prior to the recording of the embedded recording information, and

the recording device records the generated embedded start
30 information into a start information recording area that is an area on

the recording medium where the start information is to be recorded,
prior to the recording of the embedded recording information.

25. The information recording medium according to Claim 24,
5 wherein said recording program causes the recording computer to
further function as:

a detecting device for detecting the key information from the
start information recording area when recording the embedded
recording information into the recording medium; and

10 a cryptographic information encrypting device for encrypting
the cryptographic information by using the key information to
generate encrypted cryptographic information, wherein

the adding device adds the reproducing limit information and
the encrypted cryptographic information to the recording information
15 when recording the embedded recording information into the
recording medium to generate the added recording information.

26. The information recording medium according to Claim 21,
wherein said recording program causes the recording computer to
20 further function as:

a detecting device for detecting identification information
particular to each recording medium and previously recorded in the
recording medium, prior to the recording of the embedded recording
information; and

25 a key information generating device for generating key
information for encrypting cryptographic information used for
encrypting the recording information, by using the detected
identification information, wherein

the embedding device embeds the generated key information
30 on content information indicating the content of the recording

information to generate embedded content information, prior to the recording of the embedded recording information, and

the recording device records the generated embedded content information in the recording medium.

5

27. The information recording medium according to Claim 26, wherein said recording program causes the recording computer to further function as:

10 a detecting device for detecting the key information from the recording medium when recording the embedded recording information into the recording medium; and

a cryptographic information encrypting device for encrypting the cryptographic information by using the key information to generate the encrypted cryptographic information, wherein

15 the adding device adds the reproducing limit information and the encrypted cryptographic information to the recording information to generate the added recording information, when recording the embedded recording information into the recording medium.

20 28. An information recording medium in which a reproducing control program is recorded in a readable way by a reproducing computer included in an information reproducing apparatus for reproducing recording information, which is encrypted and recorded with an reproducing limit information for controlling reproducing
25 manner of the recording information in a recording medium, based on the reproducing limit information, said reproducing limit information which is added to the recording information and also embedded on the recording information in a way of preventing from illegal detection, said reproducing program causing the reproducing
30 computer to function as:

a reproducing limit information detecting device for detecting the added reproducing limit information;

a reproducing limit information extracting device for extracting the embedded reproducing limit information from the recording information;

a recording information extracting device for extracting original recording information from the recording information on which the reproducing limit information is embedded; and

an output control device for, only when the detected reproducing limit information matches the extracted reproducing limit information, supplying the extracted original recording information based on the reproducing limit information.

29. The information recording medium, according to Claim 28, wherein

said recording medium having a start information recording area, said start information recording area in which start information detected at starting the reproducing of the recording information is recorded, said start information on which key information for encrypting cryptographic information used for encrypting the recording information is embedded, said key information which is generated by using identification information, said identification information particular to each recording medium and recorded in the recording medium, said cryptographic information which is encrypted by using the key information and added to the recording information to which the reproducing limit information is added,

wherein said reproducing program causes the reproducing computer to further function as:

a key information detecting device for detecting the key information from the start information recording area;

an encrypted cryptographic information detecting device for detecting the encrypted cryptographic information from the recording medium;

an obtaining device for decoding the detected encrypted cryptographic information by using the detected key information and obtaining original cryptographic information; and

a decoding device for decoding the extracted original recording information by using the obtained original cryptographic information and supplying the decoded recording information to the output control device.

30. The information recording medium according to Claim 28, wherein

said recording medium in which content information indicating the content of the recording information is recorded, said content information on which key information for encrypting cryptographic information used for encrypting the recording information is embedded, said key information which is generated by using identification information, said identification information particular to each recording medium and recorded in the recording medium, said cryptographic information which is encrypted by using the key information and added to the recording information to which the reproducing limit information is added,

wherein said reproducing program causes the reproducing computer to further function as:

a key information detecting device for detecting the key information from the recording medium;

an encrypted cryptographic information detecting device for detecting the encrypted cryptographic information from the recording medium;

an obtaining device for decoding the detected encrypted cryptographic information by using the detected key information and obtaining original cryptographic information; and

- 5 a decoding device for decoding the extracted original recording information by using the obtained original cryptographic information and supplying the decoded recording information to the output control device.